



Wireless Intercom Speaker

User Manual



Foreword

General

This manual introduces the installation, functions and operations of the Wireless Intercom Speaker (hereinafter referred to as "the speaker"). Read carefully before using the device, and keep the manual safe for future reference.

Symbols

The following symbols might appear in the manual.

Symbol	Description
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	July 2026

Privacy Protection Notice

As the device user, you might collect the personal data of individuals such as their names, email addresses, face images, audio and fingerprints. You shall be fully responsible for any activities associated with processing personal data. You commit to comply with your local privacy protection laws and regulations to protect the legitimate rights and interests of individuals, and shall implement measures which are required by applicable law, including but not limited to, providing clear and comprehensive information to individuals before processing their personal data, obtaining consent from individuals when necessary, informing individuals of the existence of the surveillance area, and providing required contact information.

Intelligent Product Usage Statement

Intelligent products utilize AI technology to effectively enhance security. The intelligent recognition and alarm functions of the product might be affected by factors such as environmental lighting, camera angles, object obstructions, and network delays, potentially leading to false alarms, missed alerts, or response delays. This intelligent product is solely intended to be used as a security assistance tool. The results from performing identification are for reference only and do not

constitute absolute guarantee of personal or property safety. Users need to combine these products with necessary physical security measures to enhance overall protection. Except as otherwise provided by laws or in the event of intentional or gross negligence on the part of the company, the company shall not be liable for any losses caused by the aforementioned factors not attributable to the company.

Interface Declaration

This manual mainly introduces the relevant functions of the device. The interfaces used in its manufacture, the procedures for returning the device to the factory for inspection and for locating its faults are not described in this manual. Please contact technical support if you need information on these interfaces.

About the Manual

- This manual is provided for general reference only. Discrepancies might exist between the product and this manual, including but not limited to printed, electronic, or any other editions.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. Specifications and documentation are subject to change without prior notice. For the latest versions, as well as legal notices, consult the printed manual, the product webpage, our official website, or scan the QR code to access the electronic edition.
- The manual will be updated as necessary to reflect product changes and applicable legal requirements. These updates will not diminish your statutory rights, nor will they remove or weaken the safety information or essential instructions provided at the time of purchase.
- Although we make every effort to ensure accuracy, errors or deviations in descriptions of functions, operations, or technical data might occur. If there is any uncertainty or controversy, we reserve the right of final explanation.
- All trademarks, registered trademarks and company names referenced in this manual are the property of their respective owners.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the intercom speaker, hazard protection, and protection of property damage. Read carefully before using the speaker, and comply with the guidelines when using it.

Operation Requirements

**DANGER**

The device or remote control contains button batteries. Do not swallow the batteries due to the risk of chemical burns.

Possible result: The swallowed button battery can cause serious internal burns and death within 2 hours.

Preventive measures (including but not limited to):

- Keep new and used batteries out of reach of children.
- If the battery compartment is not securely closed, stop using the product immediately and keep out of reach of children.
- Seek immediate medical attention if a battery is believed to be swallowed or inserted inside any part of the body.



- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.
- Only use the device within the rated power range.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Do not disassemble the device.

Installation Requirements

**WARNING**

- Strictly comply with the local electrical safety code and standards. Make sure that the ambient voltage is stable and meets the power supply requirements of the device.
- The power supply must meet the rated voltage requirements as indicated on the device label.
- If the device uses a power adapter, ensure it meets the following requirements:
 - ◇ If a power adapter was shipped with your device, we recommend you use it. If you need to buy a separate adapter, make sure it meets the following requirements.
 - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
 - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
 - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
 - ◇ Do not connect the power adapter to the device while the adapter is powered on.



- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the device to direct sunlight or heat sources.
- Do not install the device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the device.
- Connect class I electrical appliances to a power socket with protective earthing.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Introduction.....	1
1.1 Overview.....	1
1.2 Technical Specifications.....	1
2 Checklist.....	3
3 Design.....	4
3.1 Appearance.....	4
3.2 Dimensions.....	5
4 Powering On.....	6
5 Adding Speaker to the Hub.....	7
6 Installation.....	8
7 Configuration.....	9
7.1 Viewing Status.....	9
7.2 Configuring the Speaker.....	11
8 Intercom Service.....	14
8.1 App Intercom.....	14
8.1.1 Configuring Intercom on Hub.....	14
8.1.2 Configuring Intercom on Speaker.....	14
8.1.3 Intercom Commissioning.....	14
8.2 SIP Intercom.....	14
8.3 VoIP Intercom.....	15
Appendix 1 Security Commitment and Recommendation.....	17

1 Introduction

1.1 Overview

The Wireless Intercom Speaker triggers sound and light alarms when it receives alarm signals. It also offers the intercom function, which can be enabled in the DMSS and DoLink Care mobile app, making it easy for you to communicate with people on your site. The security center can also use the intercom to communicate with your site through the speaker.

1.2 Technical Specifications

Please refer to the corresponding technical specifications according to the corresponding models.

Table 1-1 Technical specifications

Type	Parameter	Description	
Port	Microphone	Yes. The pickup range is up to 5 m (16.40 ft).	
Audio and Video	Two-way Audio	Yes. The volume is up to 90 dB@10cm.	
Function	Button	1 × panic button, 1 × power button	
	Buzzer	Yes	
	Tamper Alarm	Yes	
	Remote Update	Cloud update	
	Low Battery Alarm	Yes	
	Battery Level Display	Yes	
	Signal Strength	Signal strength detection, RF-HD detection	
Technical Parameter	LED Indicator	Red, blue and green indicators	
	Scenario	Indoor	
	Operating Current	3.1 A (Max), 20 uA (Standby) (Battery 3V*2=6V); 1.2 A (Max), 13.9 mA (Standby) (DC 12V)	
	Sound and Light Alarm	Yes	
	Sound Pressure	Volume high 85db (A) 1 m	
Wireless Parameters	Carrier Frequency	DHI-ARA16-W2 (868): 865.34 MHz–868.60 MHz	DHI-ARA16-W2: 433.1 MHz–434.6 MHz
	Transmission Power	DHI-ARA16-W2 (868): Limit 25 mW	DHI-ARA16-W2: Limit 10 mW
	Communication Distance	DHI-ARA16-W2 (868): 1700 m (alarm transmission), 1700 m (intercom)	DHI-ARA16-W2: 1300 m (alarm transmission), 1000 m (intercom)

Type	Parameter	Description
	Communication Mechanism	Two-way
	Encryption Mode	AES128
	Frequency Hopping	Yes
General	Power Supply	4 × CR123A battery/9-15 VDC
	Battery Model	CR123A
	PS Type	Type B
	Standby Time	3 years (when triggered once every 2 weeks and alarms for 120 sec)
	Power Consumption	18.6 W (Max), 0.12 mW (Standby) (Battery ,3V*2=6V); 14.4 W (Max), 166.8 mW (Standby) (DC 12V)
	Operating Environment	-10 °C to +55 °C (+14 °F to +131 °F) (indoor)
	Operating Humidity	10%–90% (RH)
	Storage Temperature	–10 °C to +55 °C (+14 °F to +131 °F)
	Storage Humidity	10%–90% (RH)
	Product Dimensions	133.0 mm × 133.0 mm × 35.5 mm (5.24" × 5.24" × 1.40")
	Packaging Dimensions	170 mm × 166 mm × 55 mm (6.69" × 6.54" × 2.71")
	Installation	Wall mount
	Net Weight	377 g (0.83 lb)
	Gross Weight	507 g (1.12 lb)
	Casing	PC + ABS
	Color	White
	Anti-corrosion	Basic Protection *The products are designed for general use and are applicable even in areas with no specific requirements for anti-corrosion protection.

2 Checklist

Check the package against the following list. If any of the items are damaged or missing, contact customer service.

Figure 2-1 Checklist

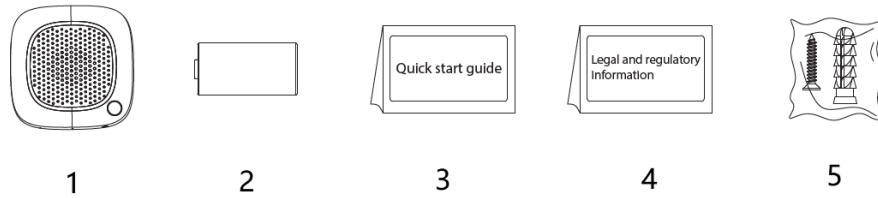


Table 2-1 Checklist

No.	Item	No.	Item
1	Wireless intercom speaker	4	Legal and regulatory information
2	CR123A battery × 4	5	Package of screws
3	Quick start guide	-	-

3 Design

3.1 Appearance

Figure 3-1 Appearance

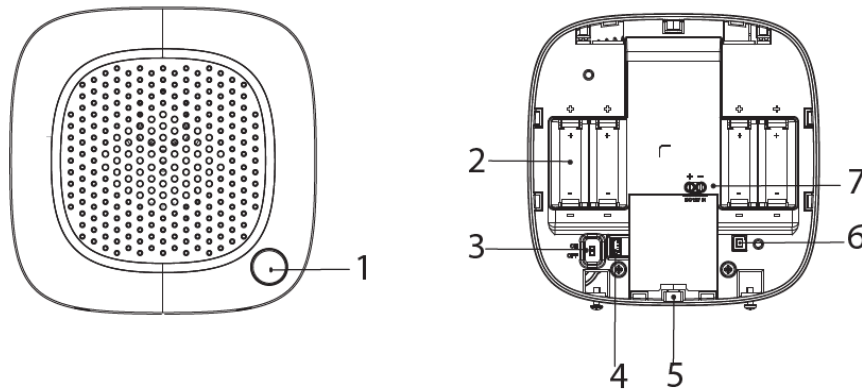
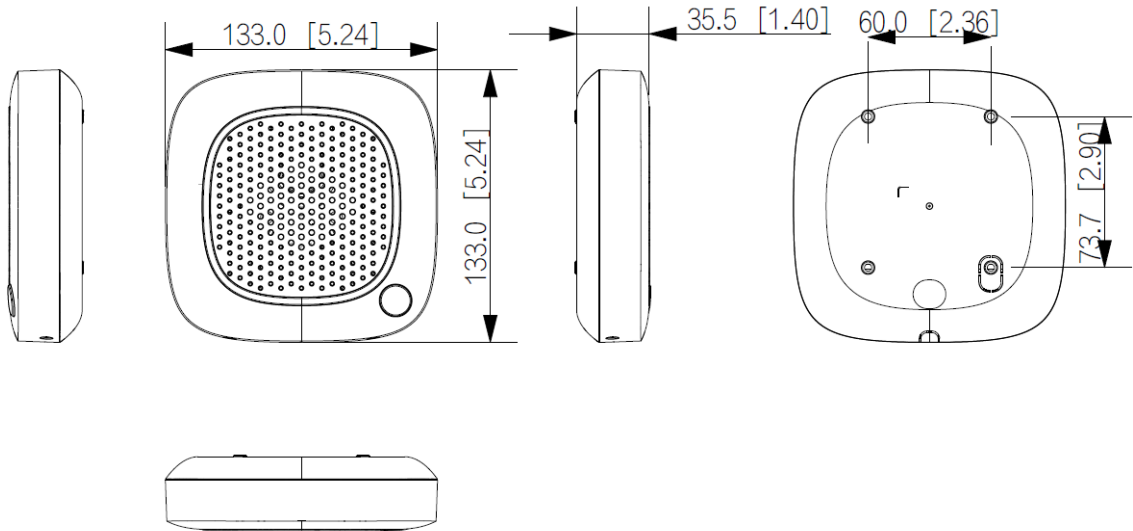


Table 3-1 Structure

No.	Name	Description
1	Panic button	Press to activate an alarm as soon as an intruder or threat is encountered.
2	Battery compartment	Used to place batteries.
3	On/off switch	Turn on or turn off the speaker.
4	Serial port	Used for debugging.
5	MIC	Captures audio.
6	Tamper switch	When the tamper switch is released, the tamper alarm will be triggered.
7	12 VDC power terminal	Insert the 12 VDC power cable.  The cable is not included in the package.

3.2 Dimensions

Figure 3-2 Dimensions (mm [inch])

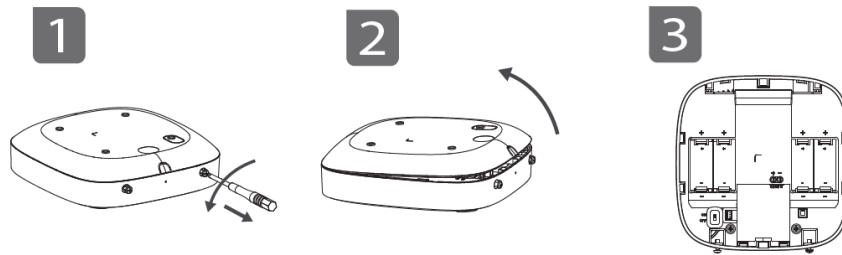


4 Powering On

Procedure

Step 1 Open the back cover of the speaker.

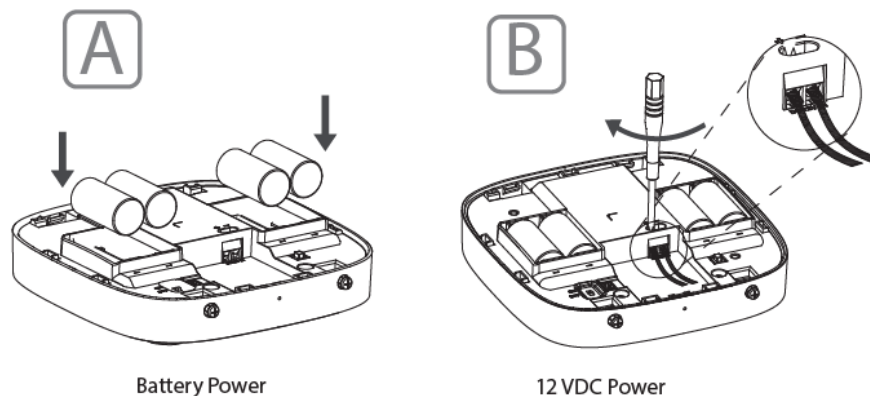
Figure 4-1 Open the front panel



Step 2 Power on the speaker through either battery or 12 VDC power.

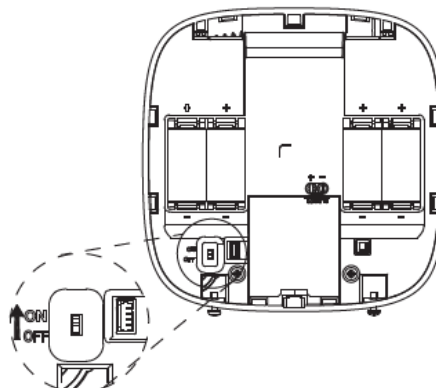
- Battery power: Install four CR123A batteries according to the polarity mark.
- 12 VDC power: Feed the 12 VDC power cable into the case through the power cable knockout.

Figure 4-2 Power on



Step 3 Push the power switch to **ON**.

Figure 4-3 Switch



5 Adding Speaker to the Hub

Background Information

Before you connect the speaker to the hub, install the DMSS app on your phone. This manual uses iOS as an example.



- Make sure that the version of the DMSS app is 2.6.0 or later, and the hub 2 is 2.000.0000010.1.R.260620 or later.
- Make sure that you have already created an account, and added the hub to DMSS.
- Make sure that the hub has a stable internet connection.
- Make sure that the hub is disarmed.

Procedure

- Step 1 Go to the hub screen, and then tap **Peripheral** to add the speaker.
- Step 2 Tap **+** to scan the QR code at the bottom of the speaker, and then tap **Next**.
- Step 3 Tap **Next** after the speaker has been found.
- Step 4 Follow the on-screen instructions and switch the speaker to on, and then tap **Next**.
- Step 5 Wait for the pairing.
- Step 6 Customize the name of the speaker, and select the area, and then tap **Completed**.

6 Installation

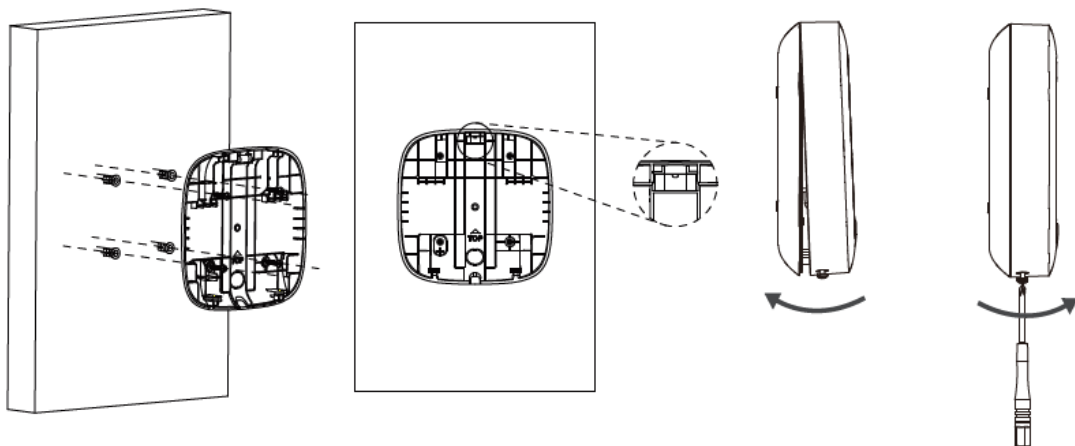
Prerequisites

Prior to installation, power on the speaker, connect it to the hub, and then perform signal strength test and RF-HD test. We recommend that you install the speaker in a place with a signal strength and RF-HD of at least 2 bars.

Procedure

- Step 1 Loosen the screw at the bottom of the speaker to remove the front panel.
- Step 2 Set the speaker into a horizontal position. Use the spirit level to make sure the speaker is horizontal and level.
- Step 3 Put the expansion bolts into the holes.
- Step 4 Align the screw holes on the rear panel with the expansion bolts.
- Step 5 Secure the rear panel with self-tapping screws.
- Step 6 Use the level to check whether the speaker is installed at a level surface.
- Step 7 Tighten the screw at the bottom of the front panel to secure the speaker.

Figure 6-1 Installation



7 Configuration

You can view and edit general information of the speaker.

7.1 Viewing Status

On the hub screen, select a speaker from the peripheral list, and then you can view the status of the speaker.

Speaker Icon Description

Introduces the meaning of icons for the speaker. You can view these icons on the hub screen.

Table 7-1 Speaker icon description

Parameter	Icon	Description
Signal Strength		Low
		Weak
		Good
		Excellent
		No signal
Bypass		Yes
		Lid only
Permanent Deactivation		Yes
		Lid only
Battery Level		100%
		80%
		60%
		40%
		20%
		No battery

Parameter	Icon	Description
Tamper		Opened
Repeater		Repeater enabled

Speaker Status Description

On the **Devices** screen of the hub, select a speaker, and then select **Overview** to view the information and status.

Table 7-2 Status

Parameter	Description
Device No.	Displays the number of the speaker.
Temperature	Displays the temperature of the speaker.  The temperature has a tolerance of $\pm 3^{\circ}\text{C}$, and the measurement accuracy is 1°C.
Signal Strength	Displays the signal strength of the speaker.
Online Status	Online and offline status of the speaker.
Battery Level	Shows the remaining electricity of the battery in the form of percentage.
Permanent Deactivation	The status for whether the permanent deactivation of the speaker is enabled or turned off. • Yes • Lid only • No
Bypass	Whether bypass is enabled or not. Once enabled, all information will not be sent to the hub. • Yes • Lid only • No
Tamper	Displays the anti-tamper status of the speaker. The types include: • Opened • Disconnected
Alarm Volume	Displays the volume status of the function. • Off • Low • Medium • High
Alarm Duration	Displays the alarm duration (sec).

Parameter	Description
Play Sound for Arming and Disarming	Displays the volume status of the function. • Off • Low • Medium • High
Play Sound for Delay Time	Displays the volume status of the function. • Off • Low • Medium • High
Doorbell	Displays the doorbell status of the speaker. • Disabled • Enabled
Repeater	The status of whether the speaker forwards peripheral messages to the hub through the repeater.
Firmware Version	Displays the latest version of the program.

7.2 Configuring the Speaker

On the hub screen, select a speaker from the peripheral list, and then tap  to configure the parameters of the speaker.

Table 7-3 Speaker parameter description

Parameter	Description
Device Configuration	• View speaker name, type, SN and device model. • Edit speaker name, and then tap Save to save your configurations.
Area	Select the area to which the speaker is assigned.
Zone No.	The zone number assigned to the speaker, which cannot be configured.
Bypass	• Yes: Bypass is enabled, and information will not be sent to the alarm hub. • Lid only: Tamper only. All information, except for tamper alarms, will be sent to the alarm hub. • No: Bypass is turned off. All information will be sent to the alarm hub.  Bypass will automatically restore after disarming.

Parameter	Description
Permanent Deactivate	- Tap Enable , and then the permanent deactivate function of speaker will be enabled. Enable is set by default. - Tap Only Disable Tamper Alarm, and then the system will only ignore tamper alarm messages. - Tap Disable, and then the permanent deactivate function of the speaker will be disabled.
Control Permissions	Select areas to which the speaker will be linked when an alarm is triggered.
Status LED	Status LED is enabled by default.  If Status LED is disabled, the LED indicator will remain off regardless of whether the speaker is functioning normally or not.
Sound Settings	Alarm Volume : Configure alarm volume level of the speaker sound. Select from Off, Low, Medium and High. Doorbell : Enable the function to configure the ringtone audios. You can upload audios and link devices. Play Sound for Arming and Disarming /Play Sound for Delay Time: Enable the function, and the speaker plays sound when it is armed/disarmed/enter delay time. Volume : Set the volume of the speaker sound when it is armed/disarmed/enter delay time. Select from , Low, Medium and High.
Alarm Duration	Configure the duration of the alarm sound.
Arm Indication	Enable the Arm Indication function if you need. The system's arming status will only be indicated when the external power supply is connected correctly after enabling the function.
Alarm Status Indication	If Alarm Status Indication is enabled, the LED indicator will turn on when an alarm is triggered in an armed area. The LED indicator will flash twice every minute if an area has not been disarmed, and an alarm event ended 30 seconds in advance.  The indicator works when only main power is enabled.
Over-temperature Alarm	Enable the Over-temperature Alarm function, and then the alarm will be triggered when the temperature of the area where the detector is installed is higher or lower than the defined one. Tap  next to Over-temperature Alarm to enable this function. Scroll left and right on the temperature bar to set the lowest temperature or highest temperature, or tap + or - to set the temperature ranges.

Parameter	Description
Panic Button	● Panic Button : Enable the function and press and hold the button on the front panel of the speaker for 5 seconds, alarm messages will be reported. ● Link Alarm to Siren : When an alarm is triggered, the alarm events are reported with siren linkages. ● Alarm and Video Linkage : When an alarm is triggered, the alarm events are reported with videos. ● Video Channel : Select the video channel to be linked after pressing the panic button.
External Power Detection	If External Power Detection is enabled, power failure alarm messages will be pushed to the DMSS.
Intercom Service	Intercom between speaker and DMSS app, or between speaker and third-party SIP platform. Enable the function, and the speaker can achieve the intercom function.
Signal Strength Detection	Check the current signal strength.
RF-HD Test	Tap Start Detection to test the RF-HD signal of the location where the speaker is placed.
Siren Test	Tap Start Detection to test whether the buzzer works normally. The speaker sounds for 5 seconds during the test.
Transmit Power	● Select from high, low, and automatic. ● The higher transmission power levels are, the further transmissions can travel, but power consumption increases.
Cloud Update	Update online.

8 Intercom Service

8.1 App Intercom

8.1.1 Configuring Intercom on Hub

You need to configure the intercom services on the hub.

On the **Hub** screen, select **Hub Setting** > **Intercom Service**, and enable **Intercom Service**.

Table 8-1 Intercom setting

Parameter	Description
Intercom Time Limit	When an alarm is triggered, intercom services can be initiated within the configured time interval. Once the time goes expired, a new intercom session cannot be started again.  The duration of every intercom session cannot be over 15 minutes.
Intercom	App Intercom: Intercom between the speaker and DMSS app. Select the speaker assigned to different areas.

8.1.2 Configuring Intercom on Speaker

Go to the **Device Details** page of the intercom speaker, and then tap , and enable **Intercom Service**.

8.1.3 Intercom Commissioning

Initiate an intercom session through DMSS app.

Procedure

- Step 1 On the home screen, select **Message**.
- Step 2 Tap an alarm message reported by the speaker, and then tap initiate the intercom session.

8.2 SIP Intercom

You need to configure the intercom services on the hub, and then enable **Intercom Service** on the configuration screen of the speaker.

On the **Hub** screen, select **Hub Setting** > **Intercom Service**, and enable **Intercom Service**.

Table 8-2 Intercom setting

Parameter	Description
Intercom Time Limit	When an alarm is triggered, intercom services can be initiated within the configured time interval. Once the time goes expired, a new intercom session cannot be started again.  The duration of every intercom session cannot be over 15 minutes.
Intercom	SIP Intercom: Intercom between the speaker and third party platform through SIP. ● SIP Intercom : Select the speaker for intercom. You can select Select by Siren or Select by Zone. ● Server Config : ◇ Username /Password: Subject to configuration in third-party platform. ◇ SIP Server Address : Enter the IP address of the third party platform. ◇ SIP Server Port /Local Port: Be consistent with port number of third party platform. ◇ Registration Status : Displays the status for whether the SIP is configured or not.

8.3 VoIP Intercom

You need to configure the intercom services on the hub, and then enable **Intercom Service** on the configuration screen of the speaker.

On the **Hub** screen, select **Hub Setting** > **Intercom Service**, and enable **Intercom Service**.

Table 8-3 Intercom setting

Parameter	Description
Intercom Time Limit	When an alarm is triggered, intercom services can be initiated within the configured time interval. Once the time goes expired, a new intercom session cannot be started again.  The duration of every intercom session cannot be over 15 minutes.

Parameter	Description
Intercom	VoIP Intercom: Intercom between the speaker and third party platform through VoIP. ● VoIP Intercom : Select the speaker for intercom. You can select Select by Siren or Select by Zone. ● Server Config : ◇ Device ID : Enter the device ID of the server. ◇ Username /Password: Subject to configuration in the server. ◇ Server Address : Enter the IP address of the server. ◇ Server Port /Local Port: Be consistent with port number of the server. ◇ Wait Time for Answer : Select the wait time from the list.

Appendix 1 Security Commitment and Recommendation

Zhejiang Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

Account Management

1. Use complex passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters: upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use repeating characters, such as 111, aaa, etc.

2. Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. Enable account lockout function

The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. Set and update password reset information in a timely manner

Dahua device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. Enable HTTPS

It is recommended that you enable HTTPS to access Web services through secure channels.

2. Encrypted transmission of audio and video

If your audio and video data contents are very important or sensitive, we recommend you to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

3. Turn off non-essential services and use safe mode

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up complex passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.

4. Change HTTP and other default service ports

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. Enable Allowlist

It is recommended that you turn on the allowlist function, and only allow IP in the allowlist to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allowlist.

2. MAC address binding

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3. Build a secure network environment

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
- According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
- Establish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. Check online users

It is recommended to check online users regularly to identify illegal users.

2. Check device log

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

We recommend you to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188